# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-288522
(43)Date of publication of application : 31.10.1995

(51)Int.Cl. H04L 9/34
H04K 1/06

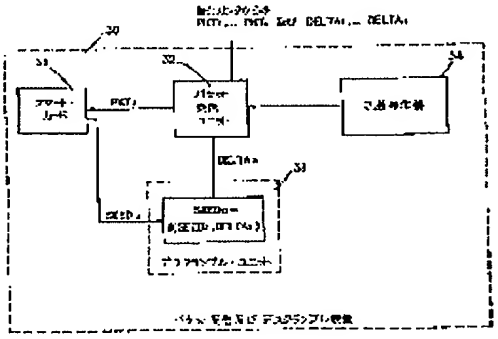
(21)Application number : 06-306465
(22)Date of filing : 09.12.1994

(71)Applicant : NEWS DATACOM LTD
(72)Inventor : NACHMAN JACOB B
TSURIA YOSSEF

(30)Priority
Priority number : 93 107967 Priority date : 09.12.1993 Priority country : IL

## (54) SYSTEM AND METHOD FOR PREVENTING HACKING

(57)Abstract:
PURPOSE: To prevent enciphered data from a transmitter from being deciphered by an unauthorized receiver in a network system.
CONSTITUTION: When a packet reception unit 32 receives packets PKT1-PKTn and offsets DELTA1-DELTAn from the transmitter and a random number from a random number generator 34 is '3', for example, the packet PKT3 is supplied to a smart card 36 and the offset DELTA3 is supplied to a descramble unit 38. The smart card calculates a seed SEED3 corresponding to the supplied packet and supplies it to the descramble unit. The descramble unit calculates a seed SEED0 based on the supplied SEED3 and offset DELTA3 and descrambles the received data while using the provided seed. Since descrambling is enabled only when the seed from the smart card is suitable, deciphering at the non-permitted receiver is prevented.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

**特開平7－288522**

(43)公開日　平成７年(1995)10月31日

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ | 技術表示箇所 |
|---|---|---|---|---|
| Ｈ０４Ｌ　9/34 | | | | |
| Ｈ０４Ｋ　1/06 | | | | |
| | | | Ｈ０４Ｌ　9/ 00 | Ｂ |

審査請求　未請求　請求項の数32　ＯＬ　（全 10 頁）

(21)出願番号　特願平6－306465

(22)出願日　平成６年(1994)12月９日

(31)優先権主張番号　１０７９６７

(32)優先日　1993年12月９日

(33)優先権主張国　イスラエル（ＩＬ）

(71)出願人　594146065
ニューズ・データコム・リミテッド
ＮＥＷＳ　ＤＡＴＡＣＯＭ　ＬＴＤ
イギリス国ロンドン　イー１・９エックスワイ，ヴァージニア・ストリート，ピー・オー・ボックス　495

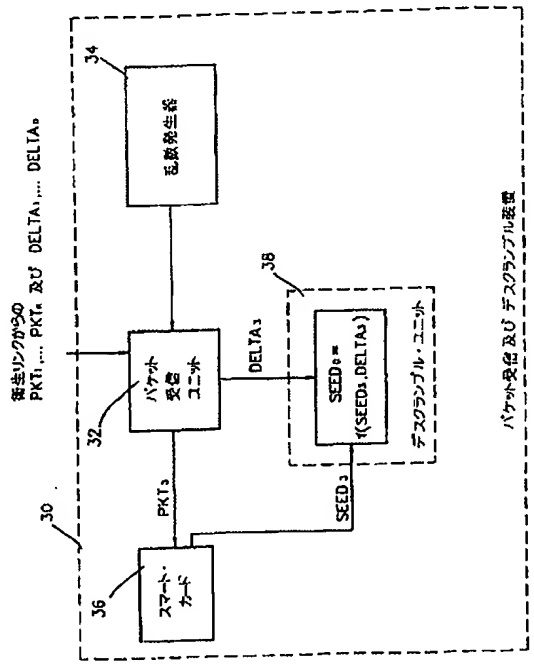
(72)発明者　ジェイコブ・ベザレル・ナックマン
イスラエル国　ラマット・モディーム　73127，ハタマール・ストリート　3

(72)発明者　ヨゼフ・ツーリア
イスラエル国　エルサレム　97276，シャローム・シヴァン・ストリート　20

(74)代理人　弁理士　湯浅　恭三　（外６名）

(54)【発明の名称】　ハッキング防止システム及び方法

(57)【要約】
【目的】ネットワーク・システムにおいて、送信機からの暗号化されたデータが無許可受信機で非暗号化されないようにする。
【構成】送信機からのデータ・パケットＰＫＴ1～ＰＫＴn及びオフセットＤＥＬＴＡ1～ＤＥＬＴＡnをパケット受信ユニット３２が受信すると、乱数発生器３４からの乱数が例えば“３”のとき、パケットＰＫＴ3をスマート・カード３６に供給し、かつオフセットＤＥＬＴＡ3をデスクランブル・ユニット３８に供給する。スマート・カードは供給されたパケットに対応するシードＳＥＥＤ3を計算してデスクランブル・ユニットに供給する。デスクランブル・ユニットは、供給されたシードＳＥＥＤ3及びオフセットＤＥＬＴＡ3に基づいてシードＳＥＥＤ0を計算し、該得られたシードを用いて受信されたデータをデスクランブルする。スマート・カードからのシードが適切な場合にのみデスクランブルスルが可能なので、無許可受信機での解読が防止される。



【特許請求の範囲】

【請求項１】　ネットワークにおけるハッキング防止システムであって、該ネットワークが、１つの送信機と、それぞれがシークレット・ナンバーによって独立にイネーブルされ、かつイネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を非暗号化する複数の受信機とを含んでいるハッキング防止システムにおいて、前記受信機のそれぞれは、

前記データの少なくとも一部と、前記受信機の中の複数のものに関して異なっている関数手段とを用いて、異なる関数手段を有するそれぞれの受信機に関して異なっている第１のキーを発生する第１のキー発生器と、

前記データの少なくとも一部と前記関数手段とを用いて、第２のキーを生じる第２のキー発生器と、

前記第２のキーとともに前記第１のキーを利用して、前記複数の受信機のすべてにおいて同一である前記シークレット・ナンバーを生じるシークレット・ナンバー発生器とを備えており、ある受信機において傍受された第１及び第２のキーが、異なる関数手段を有する別の受信機をイネーブルすることができないようにしたことを特徴とするハッキング防止システム。

【請求項２】　請求項１記載のハッキング防止システムにおいて、前記受信機の少なくとも複数のものに関して異なっている前記関数手段は、乱数発生器によってその値が規定されることを特徴とするハッキング防止システム。

【請求項３】　請求項１記載のハッキング防止システムにおいて、前記第２のキー発生器は、単一のＶＬＳＩチップとして形成されていることを特徴とするハッキング防止システム。

【請求項４】　請求項３記載のハッキング防止システムにおいて、前記単一のＶＬＳＩチップは、スマート・カード上に配置されていることを特徴とするハッキング防止システム。

【請求項５】　請求項１記載のハッキング防止システムにおいて、前記第１のキー発生器、前記関数手段、及び前記シークレット・ナンバー発生器は、単一のＶＬＳＩチップとして構築されていることを特徴とするハッキング防止システム。

【請求項６】　請求項１記載のハッキング防止システムにおいて、前記第１のキー発生器、前記関数手段、前記シークレット・ナンバー発生器、及び前記第２のキー発生器は、単一のＶＬＳＩチップとして構築されていることを特徴とするハッキング防止システム。

【請求項７】　請求項６記載のハッキング防止システムにおいて、前記受信機のそれぞれは、前記ＶＬＳＩチップの少なくとも１つを有していることを特徴とするハッキング防止システム。

【請求項８】　請求項１記載のハッキング防止システムにおいて、前記ネットワークはＣＡＴＶネットワークであり、前記受信機はＣＡＴＶ受信及びデコーダとであることを特徴とするハッキング防止システム。

【請求項９】　１つの送信機と、それぞれがシークレット・ナンバーによって独立にイネーブルされ、かつイネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を解読する複数の受信機と、を含むネットワークにおいて用いられるハッキング防止方法において、

前記データの少なくとも一部と前記受信機の中の少なくとも複数のものに関して異なる関数手段とを用いることによって、異なる関数手段を有するそれぞれの受信機に関して異なっている第１のキーを発生するステップと、

前記データの少なくとも一部と前記関数手段とを用いることによって、第２のキーを生じるステップと、

前記第２のキーと共に前記第１のキーを利用して、前記受信機のすべてに関して同一である前記シークレット・ナンバーを生じることによって、シークレット・ナンバーを発生するステップとを含んでおり、ある受信機において傍受された第１及び第２のキーが、異なる関数手段を有する別の受信機をイネーブルすることができないようにしたことを特徴とするハッキング防止方法。

【請求項１０】　請求項９記載のハッキング防止方法において、前記受信機の少なくとも複数のものに関して異なっている前記関数手段は、乱数発生器であることを特徴とするハッキング防止方法。

【請求項１１】　請求項９記載のハッキング防止方法において、前記第２のキーの発生は、単一のＶＬＳＩチップによって実行されることを特徴とするハッキング防止方法。

【請求項１２】　請求項１１記載のハッキング防止方法において、前記単一のＶＬＳＩチップは、スマート・カード上に配置されていることを特徴とするハッキング防止方法。

【請求項１３】　請求項９記載のハッキング防止方法において、前記第１のキーの発生、前記関数手段の適用、及び前記シークレット・ナンバーの発生は、単一のＶＬＳＩチップによって実行されることを特徴とするハッキング防止方法。

【請求項１４】　請求項９記載のハッキング防止方法において、前記キーの発生と、シークレット・ナンバーを生じる前記キーの組み合わせとは、単一のＶＬＳＩチップによって実行されることを特徴とするハッキング防止方法。

【請求項１５】　請求項９記載のハッキング防止方法において、前記第１のキーの発生、前記関数手段の適用、及び前記シークレット・ナンバーの発生は、すべて、前記受信機のそれぞれにおいて実行されることを特徴とするハッキング防止方法。

【請求項１６】　請求項９記載のハッキング防止方法において、該方法はＣＡＴＶネットワークにおいて用いら

れ、前記キーの少なくとも一部と前記シークレット・ナンバーとの発生は、ＣＡＴＶ受信機とデコーダとにおいて実行されることを特徴とするハッキング防止方法。

【請求項１７】　加入者は、情報供給者、地理的位置、及び人口統計から成るパラメータの少なくとも１つによって個別に特徴付けられ、情報が、前記パラメータの少なくとも１つに従って各グループが前記情報の少なくとも一部分を受け取る権利を有している、それぞれのグループへと分類される複数の加入者に対して、情報源から送信され、１つの送信機と、それぞれが一人の加入者と関係しておりシークレット・ナンバーによって独立にイネーブルされ、イネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を解読する複数の受信機と、を含むネットワークにおいて用いられる、複数の加入者へ情報を選択的に送信する送信システムにおいて、前記受信機のそれぞれは、

前記データの少なくとも一部と前記受信機の中の少なくとも複数のものに関して異なる関数手段とを用い、異なる関数を有するそれぞれの受信機に関して異なっている第１のキーを発生する第１のキー発生器と、

前記データの少なくとも一部と前記関数手段とを用いて、第２のキーを生じる第２のキー発生器と、

前記データの少なくとも一部を用いて、前記パラメータの少なくとも１つによって特徴付けられる第３のキーを生じる第３のキー発生器と、

前記第１のキー、前記第２のキー、及び前記第３のキーを利用し、前記受信機のすべてに関して同一である前記シークレット・ナンバーを生じるシークレット・ナンバー発生器とを備えており、よって、ある受信機において傍受された第１及び第２のキーが、異なる関数手段を有する別の受信機をイネーブルすることができず、かつ、受信機のあるグループ内の受信機において傍受された第３のキーが、別のグループの受信機をイネーブルする事ができないようにしたことを特徴とする複数の加入者への情報の選択的送信システム。

【請求項１８】　請求項１７記載のシステムにおいて、前記受信機の少なくとも複数のものに関して異なっている前記関数手段は、乱数発生器であることを特徴とするシステム。

【請求項１９】　請求項１７記載のシステムにおいて、前記第２のキー発生器は、単一のＶＬＳＩチップによって形成されていることを特徴とするシステム。

【請求項２０】　請求項１９記載のシステムにおいて、前記単一のＶＬＳＩチップは、スマート・カード上に配置されていることを特徴とするシステム。

【請求項２１】　請求項１７記載のシステムにおいて、前記第１のキー発生器、前記関数手段、前記第３のキー発生器、及び前記シークレット・ナンバー発生器は、単一のＶＬＳＩチップによって形成されていることを特徴とするシステム。

【請求項２２】　請求項１７記載のシステムにおいて、前記第１のキー発生器、前記関数手段、前記第３のキー発生器、前記シークレット・ナンバー発生器、及び前記第２のキー発生器は、単一のＶＬＳＩチップによって形成されていることを特徴とするシステム。

【請求項２３】　請求項２２記載のシステムにおいて、前記受信機のそれぞれは、前記ＶＬＳＩチップの少なくとも１つを有していることを特徴とするシステム。

【請求項２４】　請求項１７記載のシステムにおいて、前記ネットワークはＣＡＴＶネットワークであり、前記受信機はＣＡＴＶ受信及びデコーダであることを特徴とするシステム。

【請求項２５】　加入者が、情報供給者、地理的位置、及び人口統計から成るパラメータの少なくとも１つによって個別に特徴付けられ、情報が、前記パラメータの少なくとも１つに従って各グループが前記情報の少なくとも一部分を受け取る権利を有している個別のグループへと分類される複数の加入者に、情報源から送信され、１つの送信機と、それぞれが一人の加入者と関係しておりシークレット・ナンバーによって独立にイネーブルされ、イネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を解読する複数の受信機と、を含むネットワークにおいて用いられる、複数の加入者への情報の選択的送信方法において、

前記データの少なくとも一部と前記受信機の中の少なくとも複数のものに関して異なっている関数手段とを用い、異なる関数手段を有するそれぞれの受信機に関して異なっている第１のキーを発生するステップと、

前記データの少なくとも一部と前記関数手段とを用いて、第２のキーを生じるステップと、

前記データの少なくとも一部を用い、前記パラメータの少なくとも１つによって特徴付けられるキーである第３のキーを発生するステップと、

前記第１のキー、前記第２のキー、及び前記第３のキーを利用し、前記受信機のすべてに関して同一である前記シークレット・ナンバーを生じることによって、シークレット・ナンバーを発生するステップとを含んでおり、ある受信機において傍受された第１及び第２のキーは、異なる関数手段を有する別の受信機をイネーブルすることができず、また、あるグループの受信機において傍受された第３のキーが、別のグループの受信機をイネーブルすることができないことを特徴とする送信方法。

【請求項２６】　請求項２５記載の方法において、前記受信機の少なくとも複数のものに関して異なっている前記関数手段は、乱数発生器であることを特徴とする方法。

【請求項２７】　請求項２５記載の方法において、前記第２のキーの発生は、単一のＶＬＳＩチップにおいて実行されることを特徴とする方法。

【請求項２８】　請求項２７記載の方法において、前記

単一のＶＬＳＩチップは、スマート・カード上に配置されていることを特徴とする方法。

【請求項２９】　請求項２５記載の方法において、前記第１のキーの発生、前記関数手段の適用、前記第３のキーの発生、及び前記シークレット・ナンバーの発生は、単一のＶＬＳＩチップにおいて実行されることを特徴とする方法。

【請求項３０】　請求項２５記載の方法において、前記キーの発生と、シークレット・ナンバーを生じるための前記キーの組み合わせとは、単一のＶＬＳＩチップにおいて実行されることを特徴とする方法。

【請求項３１】　請求項２５記載の方法において、前記第１のキー発生、前記関数手段の適用、前記キーの選択、及び前記シークレット・ナンバーの発生は、すべて、前記受信機のそれぞれにおいて実行されることを特徴とする方法。

【請求項３２】　請求項２５記載の方法において、該方法は、ＣＡＴＶネットワークにおいて用いられ、前記キーの少なくとも一部と前記シークレット・ナンバーとの前記発生は、ＣＡＴＶ受信及びデコーダにおいて実行されることを特徴とする方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、一般には、秘密（ｓｅｃｕｒｅ）通信システムに関し、更に詳しくは、暗号化された情報を１つの場所から保護されていない場所にある複数の端末へ送信するための通信システムに関する。

【０００２】

【発明の背景】秘密通信システムにおける主な問題は、無許可の侵入（ｕｎａｕｔｈｏｒｉｚｅｄ　ｐｅｎｅｔｒａｔｉｏｎ）である。この種の無許可侵入は、ハッキングと称される。ハッキングの問題を克服するために、いくつもの方法が用いられてきた。送信データの暗号化と通信者の認証とは、ハッキングをより困難にするのに用いられる方法である。克服が困難であると考えられているハッキングの方法の１つに、「マコーマック・ハッキング（ＭｃＣｏｒｍａｃ　Ｈａｃｋ）」と呼ばれるものがある。この方法は、ＣＡＴＶシステムに理論的には応用可能であると信じられており、Ｆｒａｎｋ　Ｂａｙｌｉｎ等による“Ｗｏｒｌｄ　Ｓａｔｅｌｌｉｔｅ　ＴＶ　ａｎｄ　Ｓｃｒａｍｂｌｉｎｇ　Ｍｅｔｈｏｄｓ”（Ｂａｙｌｉｎ　Ｐｕｂｌｉｃａｔｉｏｎ　第２版、１９９１年、ｐｐ．２４３～２４４）と、“Ｓａｔｅｌｌｉｔｅ　Ｗａｔｃｈ　Ｎｅｗｓ”（１９９１年８月）に記載されている。この方法によれば、正当に許可されたデコーダからのデータ・ストリームがリアルタイムで抽出され、小型の無線周波数（ＲＦ）送信機を用いて空中を送信される。そして、このデータ・ストリームを用いて、複数の海賊（ｐｉｒａｔｅ）デコーダを付勢する。

【０００３】

【発明の概要】上記した従来例に鑑み、本発明は、正当に許可を得た端末からのデータ・ストリームを抽出して、該データ・ストリームを複数の海賊端末へ送信する可能性を、実質的に防止する方法及びシステムを提供することを目的とする。本発明においては、すべての形式における用語「端末（ｔｅｒｍｉｎａｌ）」は、通常の意味よりも広く用いられており、あらゆるタイプのコンピュータ端末、ＣＡＴＶデコーダ、遠隔のコンピュータ、及び遠隔のコンピュータ化されたステーションをカバーする。本発明においては、すべての形式における用語「シード（ｓｅｅｄ）」及び「キー（ｋｅｙ）」は、通常の意味よりも広く交互に用いられており、データを暗号化／解読（すなわち、スクランブル／デスクランブル）するための暗号化／解読キーの少なくとも一部として用いられる、秘密あるいは秘密ではない、あらゆるタイプ又は他の記号（ｓｙｍｂｏｌ）をカバーする。さらに本発明においては、用語「シークレット・ナンバー」が、本発明の目的のために、データの暗号化／解読（すなわち、スクランブル／デスクランブル）のために用いられる秘密のキーを表すために用いられる。

【０００４】本発明の好適実施例によれば、１つの送信機とそれぞれがシークレット・ナンバーによって独立にイネーブルされ（使用可能状態とされ）、イネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を解読する複数の受信機とを含むネットワークにおいて用いられるハッキング防止システムであって、前記複数の受信機のそれぞれは、前記データの少なくとも一部と前記複数の受信機の中の少なくとも複数のものに対して異なる関数とを用い、異なる関数を有するそれぞれの受信機に対して異なっている第１のキーを発生する第１のキー発生器と、前記データと前記関数との少なくとも一部を用いて第２のキーを生じる第２のキー発生器と、前記第２のキーと共に前記第１のキーを利用し前記複数の受信機のすべてに対して同一である前記シークレット・ナンバーを生じるシークレット・ナンバー発生器とを備えており、これにより、第１の受信機において傍受された第１及び第２のキーにより、異なる関数を有する第２の受信機をイネーブルすることができないように構成された、ハッキング防止システムが提供される。

【０００５】本発明の別の好適実施例によれば、１つの送信機とそれぞれがシークレット・ナンバーによって独立にイネーブルされイネーブルされている場合には、前記送信機から受信されたデータに応答して、暗号化された情報を解読する複数の受信機とを含むネットワークと共に用いられるハッキング防止方法であって、前記データの少なくとも一部と前記複数の受信機の中の少なくとも複数のものに対して異なる関数とを用いることによって、異なる関数を有するそれぞれの受信機に対して異なっている第１のキーを発生するステップと、前記データ

と前記関数との少なくとも一部を用いることによって、第２のキーを生じるステップと、前記第２のキーと共に前記第１のキーを利用し、前記複数の受信機のすべてに対して同一である前記シークレット・ナンバーを生じることによって、シークレット・ナンバーを発生するステップとを含んでおり、これにより、第１の受信機において傍受された第１及び第２のキーが、異なる関数を有する第２の受信機をイネーブルすることができないように構成されたハッキング防止方法が提供される。

【０００６】更に別の本発明の好適実施例によれば、加入者が、情報供給者、地理的位置、及び人口統計から成るパラメータの少なくとも１つによって個別に特徴付けられ、前記パラメータの少なくとも１つに従って各グループが前記情報の少なくとも一部分を受け取る権利を有している異なるグループへと分類される複数の加入者に対して、情報が情報源から送信され、１つの送信機が、それぞれが一人の加入者と関連しかつシークレット・ナンバーによって独立にイネーブルされ、イネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を解読する複数の受信機とを含むネットワークにおいて用いられる、複数の加入者へ情報を選択に送信する送信システムであって、前記複数の受信機のそれぞれは、前記データの少なくとも一部と前記複数の受信機の中の少なくとも複数のものに対して異なる関数とを用い、異なる関数を有するそれぞれの受信機に対して異なっている第１のキーを発生する第１のキー発生器と、前記データと前記関数との少なくとも一部を用いて、第２のキーを生じる第２のキー発生器と、前記データの少なくとも一部を用いて、前記パラメータの少なくとも１つによって特徴付けられる第３のキーを生じる第３のキー発生器と、前記第１のキー、前記第２のキー、及び前記第３のキーを利用し、前記複数の受信機のすべてに対して同一である前記シークレット・ナンバーを生じるシークレット・ナンバー発生器とを備えており、それにより、第１の受信機において傍受された第１及び第２のキーが、異なる関数を有する第２の受信機をイネーブルすることができないように構成され、かつ受信機の第１のグループの一部を形成する受信機において傍受された第３のキーが、受信機の前記グループの第２のものの一部を形成する受信機をイネーブルすることができないように構成され、複数の加入者への情報の選択的送信システムが提供される。

【０００７】更にまた本発明の実施例によれば、加入者が、情報供給者、地理的位置、及び人口統計から成るパラメータの少なくとも１つによって個別に特徴付けられ、前記パラメータの少なくとも１つに従って各グループが前記情報の少なくとも一部分を受け取る権利を有している異なるグループへと分類される複数の加入者に、情報が情報源から送信され、１つの送信機が、それぞれが一人の加入者と関係しておりかつシークレット・ナンバーによって独立にイネーブルされ、イネーブルされている場合には前記送信機から受信されたデータに応答して暗号化された情報を解読する複数の受信機とを含むネットワークにおいて用いられる、複数の加入者へ情報を選択的に送信する送信方法であって、前記データの少なくとも一部と前記複数の受信機の中の少なくとも複数のものに対して異なる関数とを用い、異なる関数を有するそれぞれの受信機に対して異なっている第１のキーを発生するステップと、前記データと前記関数との少なくとも一部を用いて、第２のキーを生じるステップと、前記データの少なくとも一部を用い、前記パラメータの少なくとも１つによって特徴付けられるキーを生じることによって、第３のキーを発生するステップと、前記第１のキー、前記第２のキー、及び前記第３のキーを利用し、前記複数の受信機のすべてに対して同一である前記シークレット・ナンバーを生じることによってシークレット・ナンバーを発生するステップとを含んでおり、それにより、第１の受信機において傍受された第１及び第２のキーが、異なる関数を有する第２の受信機をイネーブルすることができないように構成され、また、受信機の第１のグループの一部を形成する受信機において傍受された第３のキーが、受信機の前記グループの第２のものの一部を形成する受信機をイネーブルすることができないように構成されている、複数の加入者への情報の選択的送信方法が提供される。

【０００８】本発明の好適実施例によれば、前記複数の受信機の少なくとも複数のものに対して供給される異なる前記関数は、乱数発生器である。前記第２のキー発生器は、単一のＶＬＳＩチップに形成されることが好ましい。本発明の好適実施例によれば、前記ＶＬＳＩチップは、スマート・カード上に配置されている。前記第１のキー発生器、前記関数、及び前記シークレット・ナンバー発生器は、単一のＶＬＳＩチップに形成されることが好ましい。本発明の好適実施例によれば、前記第１のキー発生器、前記関数、前記シークレット・ナンバー発生器、及び前記第２のキー発生器は、単一のＶＬＳＩチップに形成される。好ましくは、前記複数の受信機のそれぞれは、前記ＶＬＳＩチップの少なくとも１つを含む。本発明の好適実施例によれば、前記ネットワークはＣＡＴＶネットワークであり、前記複数の受信機はＣＡＴＶ受信機とデコーダとで構成される。

【０００９】

【実施例】まず、図１を参照して、従来技術の「マコーマック・ハッキング」方法によって構成され動作する、理論的ハッキング・システムを説明する。通常は有効スマート・カード１２によって動作される、許可を得た（ａｕｔｈｏｒｉｚｅｄ）デコーダ（許可デコーダ）１０が、標準的なスマート・カード通信リンク１５を介してマコーマック・ハッキング・インターフェース（ＭＨＩ）ユニット１４に結合されている。スマート・カード

１２も、また、標準的なスマート・カード通信リンク１６を介してＭＨＩユニット１４に結合されている。ＭＨＩユニット１４は、スマート・カード１２と許可デコーダ１０との間で伝達される通信データの「匂いを嗅ぎ（ｓｎｉｆｆｓ）」、それを小型の無線送信機１８に与える。無線送信機１８は、データを、無線周波数（ＲＦ）リンク１９を介して、仮想スマート・カード２２に結合された無線受信機２０に送信する。仮想スマート・カード２２は、標準的なスマート・カード通信リンク２５を介して、無許可デコーダ２４に結合されている。このようにして、無許可デコーダ２４は、許可デコーダ１０を動作させるのと同じデータ・ストリームによって動作される。

【００１０】別の例では、ＭＨＩユニット１４は、許可デコーダ１０の内部のユニットの間で通信されるデータの「匂いを嗅ぐ」。この例では、ＭＨＩユニット１４は、通信リンク２７を介して、マイクロプロセッサ２８とデスクランブル・ユニット２９との間の通信バス２６にリンクされている。通信バス２６は、デスクランブルのために必要なシークレット・ナンバーである「シード（ＳＥＥＤ）」値を運ぶ。このようにして、シード値は抽出され、データのデスクランブルのために無許可デコーダに送信される。

【００１１】次に、図２を参照して、本発明の好適実施例によって構成され動作する加入者側のパケット受信及びデスクランブル装置を説明する。本発明の好適実施例においては、一連の許可パケット$PKT_1$～$PKT_n$を含むデータ・ストリームが、情報源から、衛星リンクを介して、加入者のＣＡＴＶ受信機及びデコーダ（図示せず）の一部を形成するパケット受信及びデスクランブル装置３０に送信される。一連のオフセット値$DELTA_1$～$DELTA_n$もまた、衛星リンクを介して、パケット受信及びデスクランブル装置３０に送信される。好ましくは、各パケットは、オフセット値と対になっている。パケット受信及びデスクランブル装置３０では、パケット受信ユニット（ＰＲＵ）３２が一連のパケットとオフセット値とを受信する。乱数発生器３４が、乱数アルゴリズムを使用することによって、１からｎの範囲の数をＰＲＵ３２に与える。たとえば、３の数が乱数発生器３４から発生されると、それに従って、対応するパケットすなわち$PKT_3$がスマート・カード３６に送信され、対応するオフセットすなわち$DELTA_3$が、これは内部キーとして機能するのだが、デスクランブル・ユニット３８に送信される。

【００１２】スマート・カード３６は、各パケットに対して適切なシード（ＳＥＥＤ）を生じるアルゴリズムを使用する。スマート・カード３６は、パケット$PKT_3$を受信した場合には、対応するシード$SEED_3$なるキーを生じ、これをデスクランブル・ユニット３８に与える。ＰＲＵ３２、乱数発生器３４、及びデスクランブル・ユニット３８はすべて、ＶＬＳＩチップ等の１つの保護されたチップにおいて形成されることが好ましい。このようにして、乱数及びオフセットの通信は、変更されるすなわち「匂いを嗅がれる（ｓｎｉｆｆｅｄ）」ことができなくなる。デスクランブル・ユニット３８においては、ＰＲＵ３２とスマート・カード３６とからそれぞれ受信されたキー、すなわちオフセット値$DELTA_3$とシード$SEED_3$は、次のような関数ｆによって用いられる。

【数１】 $f = f(\text{シード値}, \text{オフセット値})$

$SEED_0 = f(SEED_i, DELTA_i)$

ただし、$SEED_0$はデータのデスクランブルに必要なシークレット・ナンバーであり、ｉは１～ｎの中の任意の整数で、乱数発生器３４からの数である。したがって、ｉ＝３が選択された場合には、

【数２】 $SEED_0 = f(SEED_3, DELTA_3)$

である。

【００１３】本発明の好適実施例においては、デスクランブル・ユニット３８は、シード$SEED_0$の値を発生する点でシークレット・ナンバー発生器として機能し、また、内部キーとスマート・カードからのキーとを受け取るキー受信機としても機能する。シード$SEED_0$の値は、デスクランブル・ユニット３８によって、データをデスクランブルするのに用いられる。デスクランブル・ユニット３８がＶＬＳＩフォーマットを有している限りは、実際に不可能ではないにしても、シード$SEED_0$の値を傍受（タップ）するのは困難であると考えられる。図２のハッキング防止システムは、スマート・カードを用いていないシステムと共にでも動作し得ることを理解されたい。その場合には、パケット$PKT_1$～$PKT_n$に対応するシード値は、スマート・カードにおいて用いられているのと類似のアルゴリズムを用いることによって、たとえば、ＰＲＵ３２、乱数発生器３４、及びデスクランブル・ユニット３８などの、パケット受信及びデスクランブル装置３０の任意の適宜の１つの構成要素において作成される。乱数発生器３４からの乱数が受信されると、対応する計算されたシード値と適切なオフセット値とが、デスクランブル・ユニット３８に供給される。

【００１４】次に、図３のフローチャートを参照して、図２の装置の動作を説明する。一連のデータ・パケット$PKT_1$～$PKT_n$と一連のオフセット値$DELTA_1$～$DELTA_n$とが、衛星リンクを介して受信されている。乱数発生アルゴリズムが、インデックス数１～ｎの中の１つを計算し選択するのに用いられる。乱数発生アルゴリズムの出力は、たとえば、インデックス３である。計算されたインデックス３に対応するパケット、すなわち$PKT_3$が、スマート・カード３６に送信される。スマート・カードにおいては、シードを計算するアルゴリズムを用いて、対応するシード$SEED_3$を計算

するのに用いられる。そして、シードＳＥＥＤ3が、デスクランブル・ユニット３８に供給される。計算されたインデックス数に対応するオフセット値、すなわちＤＥＬＴＡ3は、、デスクランブル・ユニット３８に送信される。デスクランブル・ユニット３８は、シークレット・ナンバー発生機能を有しているのでそれを用いることにより、シードＳＥＥＤ3とオフセット値ＤＥＬＴＡ3とを組み合わせて、衛星送信をデスクランブルするのに用いられるシークレット・ナンバーであるＳＥＥＤ0の値を計算する。このシード及びオフセット値は、シークレット・ナンバー発生のため以外にも用いられる。

【００１５】次に、図４のフローチャートには、図２の装置の別の動作が示されている。該フローチャートは、シードの計算がスマート・カードにおいてではなく、図２のＰＲＵ３２において実行されている点を除けば、図３のものと同様である。シードの計算はＰＲＵ３２に限定されず、図２に示したパケット受信機及びデスクランブル・ユニット３０を形成する保護されたＶＬＳＩチップの任意の部分において実行され得ることを理解されたい。

【００１６】次に図５を参照するが、この図は、本発明の好適実施例による加入者ユニットの一部の一般化されたブロック図を示したものであり、異なる供給者によって供給された情報の受信機、又は、人口統計（ｄｅｍｏｇｒａｐｈｉｃｓ）や地理的な位置やそれ以外の任意のパラメータによってそれ以外の場合に相互に区別される受信機は、同じシークレット・ナンバーを用いてイネーブルされる。図５のシステムは、図２のシステムと比べて、さらに別のデータが、衛星リンクを介して情報源から受信され、パケット受信及びデスクランブル装置１３０において処理されている点を除いて、図２のものと同様である。図５のＰＲＵ１３２は、衛星リンクを介して、一連のパケットＰＫＴ1～ＰＫＴnと、上述のハッキング防止システムの一部で用いる一連の第１のオフセット値ＤＥＬＴＡ1～ＤＥＬＴＡnと、一連の第２のオフセット値ＧＡＭＭＡ1～ＧＡＭＭＡkとを受信する。

【００１７】第２のオフセット値ＧＡＭＭＡ1～ＧＡＭＭＡkは、プログラム供給者、地理的な位置、又は人口統計などの１つ又は複数の基準に基づいて、相互に区別され得る加入者受信機の別個のグループの間での区別に用いられる。このようにして、受信機の各グループは、第２のオフセット値の１つによって特徴付けられる。受信機のグループの特徴付けは、好ましくはパケット受信及びデスクランブル装置１３０における各デコーダの製造過程で入力される内部コード又は内部アルゴリズムか、又は、上述の例のようにデコーダとの最初の通信の際に１つの選択されたパラメータ又はパラメータ群に対してデコーダを有効化するスマート・カードにおけるアルゴリズムかのどちらかによって、達成され得る。したがって、このような特徴付けがなされると、各デコーダはイネーブルされ、それにより第２のオフセット値ＧＡＭＭＡ1～ＧＡＭＭＡkの中から１つだけを選択する。これとは別に（又は、これに加えて）、デコーダの特徴付けは、第１のオフセット値だけを用いても達成することができる。その場合には、異なるデコーダが、ある特定のオフセット値だけを受信し、それ以外は受信しないように設定される。このようにして、第２のオフセット値の使用を必要としないようにすることもできる。

【００１８】図５において、たとえば、デコーダがプログラム供給者を一意的に規定するオフセット値ＧＡＭＭＡ2を選択するように特徴付けられると、ＰＲＵ１３２は、該オフセット値ＧＡＭＭＡ2をデスクランブル・ユニット１３８に供給する。たとえば、乱数３が乱数発生器１３４によって発生されると、ＰＲＵ１３２は、対応するデータ・パケットＰＫＴ3をスマート・カード１３６に送信する。ＰＲＵ１３２は、また、選択された乱数すなわちインデックス３に従って、一連のオフセット値ＤＥＬＴＡ1～ＤＥＬＴＡnから１つのオフセット値、すなわちＤＥＬＴＡ3を、デスクランブル・ユニット１３８に供給する。装置がユーザに提供された際に、各グループに対する加入者のためのスマート・カードは、別のグループの加入者に対してのスマート・カードとは異なっている。すなわち、グループ毎にスマート・カードが異なっており、それは、グループ毎のスマート・カードで異なるアルゴリズムを用いることによって、区別されている。したがって、たとえば、２人の異なる情報供給者によって動作される２つのデコーダで、同じ乱数、たとえば３が選択されたとしても、同じデータ・パケットすなわちＰＫＴ3が両方のスマート・カードに送信されるが、各スマート・カードは異なるシード値すなわちＳＥＥＤ3とＳＥＥＤ3＊とをそれぞれ計算により得ることになる。

【００１９】そして上記した例においては、２つのデコーダのそれぞれが別個のプログラム供給者によって動作されるので、異なる第２のオフセット値ＧＡＭＭＡ2とＧＡＭＭＡ3とがそれぞれデスクランブル・ユニット１３８に送信される。この２つのデコーダのデスクランブル・ユニット１３８においては、シークレット・ナンバー発生は、次のようにして実行される。

【数３】ｆ＝ｆ（シード値，第１のオフセット値，第２のオフセット値）

ＳＥＥＤ0＝ｆ（ＳＥＥＤ3，ＤＥＬＴＡ3，ＧＡＭＭＡ2）

ＳＥＥＤ0＝ｆ（ＳＥＥＤ3＊，ＤＥＬＴＡ3，ＧＡＭＭＡ3）

上述の方法によれば、同じＳＥＥＤ0を用いながら、１つの情報源から生じ加入者の別々のグループに向けられた情報をデスクランブルし、同時に、ある加入者群に向けられた認識可能な情報を別の加入者群には受信できなくすることができる。

【００２０】図６のフローチャートは、図５の装置の動作が示している。一連のデータ・パケットＰＫＴ1～ＰＫＴn、一連の第１のオフセット値ＤＥＬＴＡ1～ＤＥＬＴＡn、及び一連の第２のオフセット値ＧＡＭＭＡ1～ＧＡＭＭＡkが、衛星リンクを介してパケット受信ユニット１３２で受信される。乱数発生アルゴリズムが、インデックス数１～ｎの中から１つを計算し選択するのに用いられ、乱数発生器１３４の出力が、たとえば、インデックス３である場合、パケットＰＫＴ3がスマート・カード１３６に送信される。スマート・カードにおいては、シードを計算するアルゴリズムが用いられて、対応するシードＳＥＥＤ3＊を計算する。そして、得られたシードＳＥＥＤ3＊が、デスクランブル・ユニット１３８に供給される。計算されたインデックス数３に対応する第１のオフセット値ＤＥＬＴＡ3は、パケット受信ユニット１３２からデスクランブル・ユニット１３８に供給される。供給者又は地域（ｊｕｒｉｓｄｉｃｔｉｏｎ）を識別する第２のオフセット値、たとえばＧＡＭＭＡ2もまた、デスクランブル・ユニット１３８に供給される。

【００２１】デスクランブル・ユニット１３８では、ＳＥＥＤ3＊、ＤＥＬＴＡ3、及びＧＡＭＭＡ2が、シークレット・ナンバー発生のアルゴリズムを用いることによって組み合わされ、衛星通信情報をデスクランブルするのに用いられるシークレット・ナンバーとなるシードＳＥＥＤ0の値が計算される。当業者は、本発明が以上で述べた内容に限定されないことを、理解されよう。むしろ、本発明の範囲は、冒頭の特許請求の範囲によってのみ定義される。

【図面の簡単な説明】

【図１】従来技術である「マコーマック・ハッキング」法に基づく理論的なハッキング・システムの一般化されたブロック図である。

【図２】本発明の好適実施例によって構成され動作する加入者ユニットの一部の装置のブロック図である。

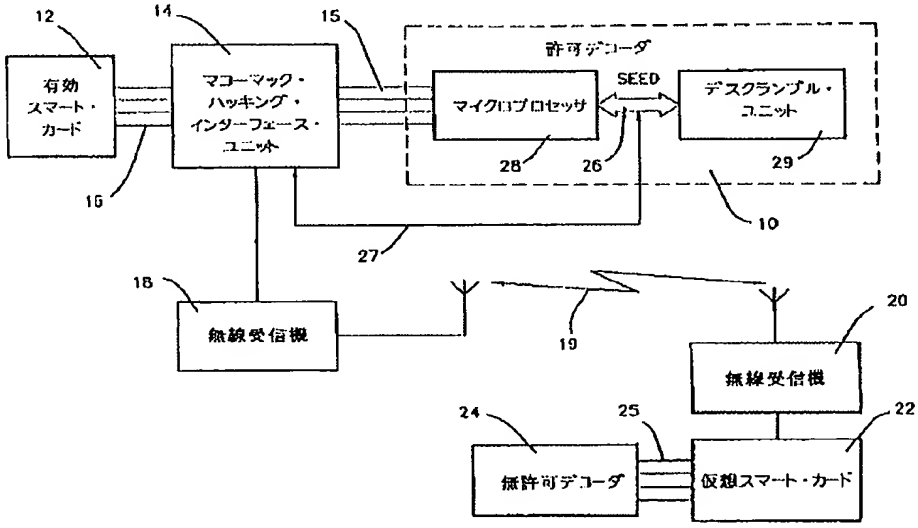
【図３】図２の装置の動作を説明するためのフローチャートである。

【図４】条件付きアクセス・カードを用いない場合の図２の装置の動作を説明するためのフローチャートである。

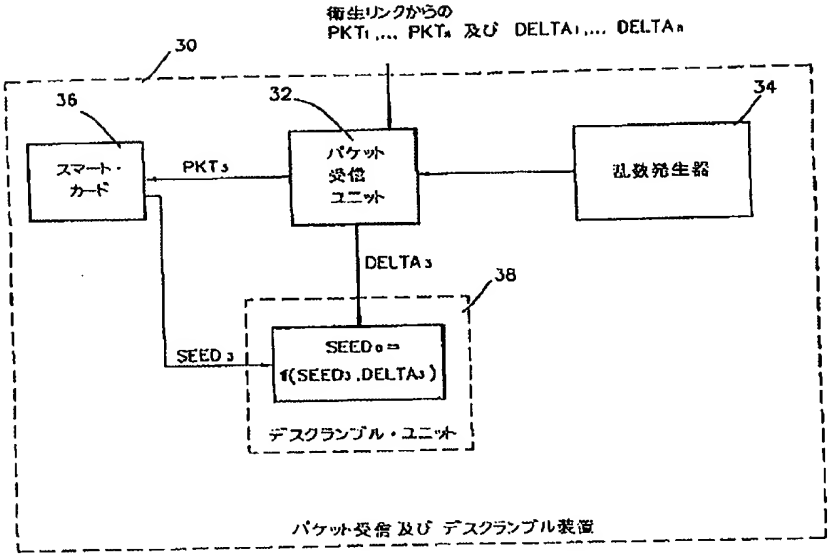
【図５】異なるパラメータによって特徴付けられる受信機を、同じシークレット・ナンバーを用いてイネーブルすることができる、本発明の好適実施例による加入者ユニットの一部の装置のブロック図である。

【図６】図５の装置の動作を説明するためのフローチャートである。

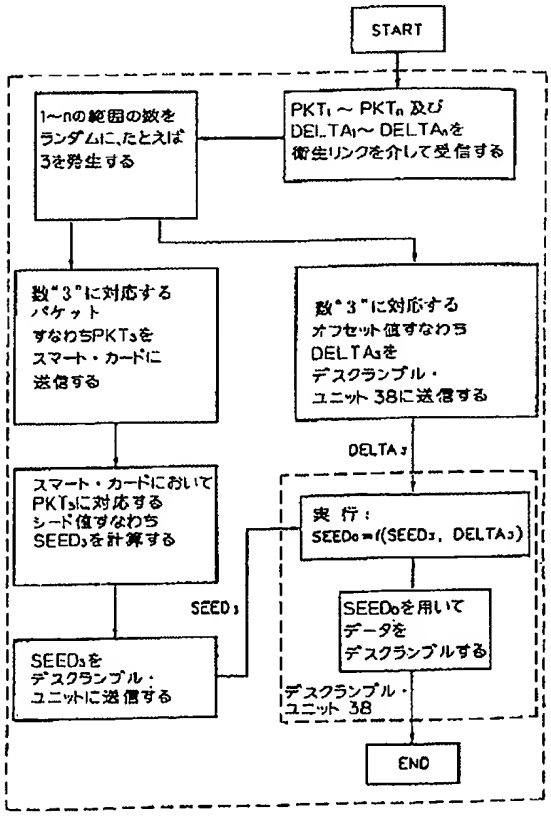
【図１】



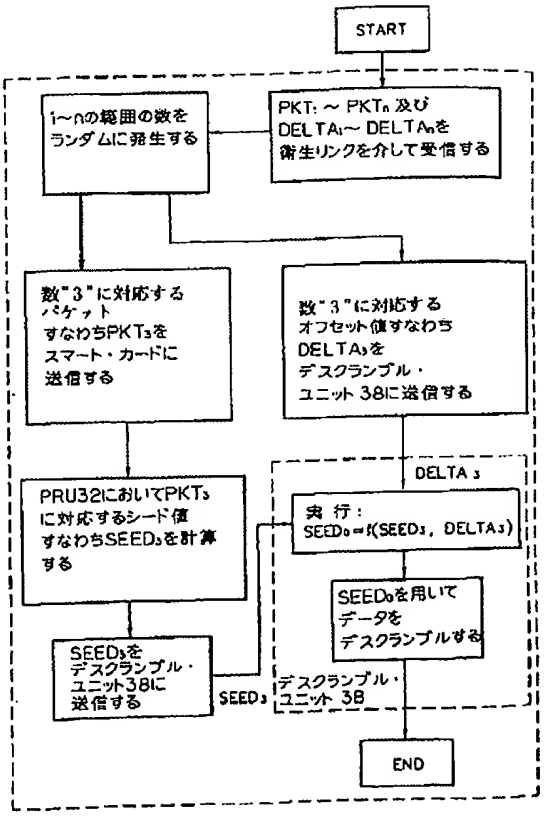
【図２】


衛生リンクからの
PKT1,... PKTn 及び DELTA1,... DELTAn
30
36
32
34
スマート・カード
PKT3
パケット受信ユニット
乱数発生器
DELTA3
38
SEED3
SEED0=f(SEED3,DELTA3)
デスクランブル・ユニット
パケット受信及びデスクランブル装置

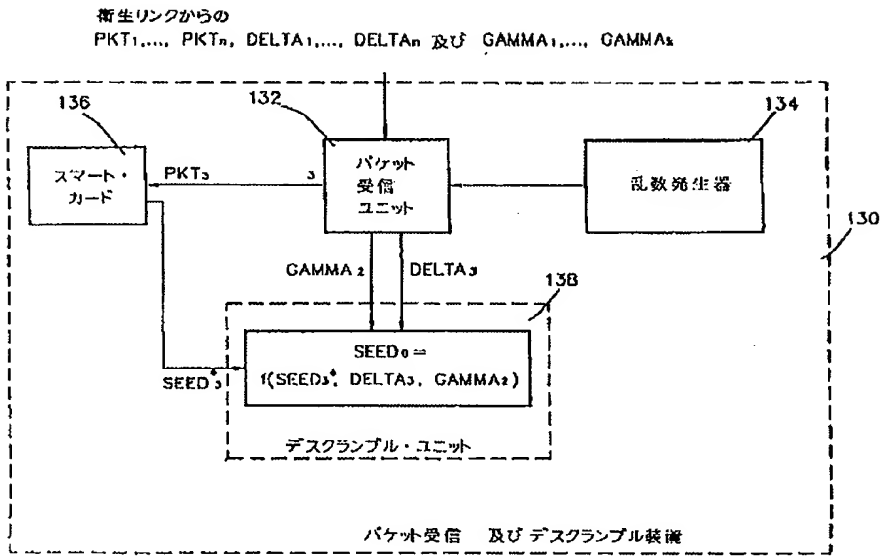
【図３】


START
1～nの範囲の数をランダムに、たとえば3を発生する
PKT1～PKTn及びDELTA1～DELTAnを衛生リンクを介して受信する
数"3"に対応するパケットすなわちPKT3をスマート・カードに送信する
数"3"に対応するオフセット値すなわちDELTA3をデスクランブル・ユニット38に送信する
DELTA3
スマート・カードにおいてPKT3に対応するシード値すなわちSEED3を計算する
実行：SEED0=f(SEED3, DELTA3)
SEED3
SEED0を用いてデータをデスクランブルする
SEED3をデスクランブル・ユニットに送信する
デスクランブル・ユニット38
END

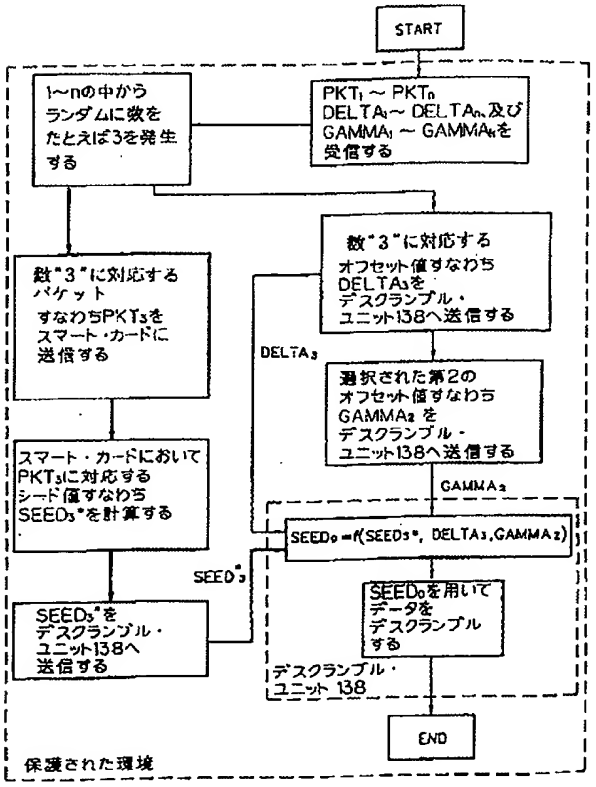
【図４】


START
1～nの範囲の数をランダムに発生する
PKT1～PKTn及びDELTA1～DELTAnを衛生リンクを介して受信する
数"3"に対応するパケットすなわちPKT3をスマート・カードに送信する
数"3"に対応するオフセット値すなわちDELTA3をデスクランブル・ユニット38に送信する
DELTA3
PRU32においてPKT3に対応するシード値すなわちSEED3を計算する
実行：SEED0=f(SEED3, DELTA3)
SEED0を用いてデータをデスクランブルする
SEED3をデスクランブル・ユニット38に送信する
SEED3
デスクランブル・ユニット38
END

【図５】


衛生リンクからの
PKT1,..., PKTn, DELTA1,..., DELTAn 及び GAMMA1,..., GAMMAk
136
132
134
スマート・カード
PKT3
パケット受信ユニット
乱数発生器
130
GAMMA 2
DELTA 3
138
SEED0 = f(SEED3*, DELTA3, GAMMA2)
SEED*3
デスクランブル・ユニット
パケット受信 及び デスクランブル装置

【図６】


START
1~nの中からランダムに数をたとえば3を発生する
PKT1 ~ PKTn
DELTA1 ~ DELTAn,及び
GAMMA1 ~ GAMMAkを
受信する
数"3"に対応するパケット
すなわちPKT3を
スマート・カードに
送信する
数"3"に対応する
オフセット値すなわち
DELTA3を
デスクランブル・
ユニット138へ送信する
DELTA3
選択された第2の
オフセット値すなわち
GAMMA2 を
デスクランブル・
ユニット138へ送信する
GAMMA2
スマート・カードにおいて
PKT3に対応する
シード値すなわち
SEED3*を計算する
SEED0 = f(SEED3*, DELTA3,GAMMA2)
SEED*3
SEED3*を
デスクランブル・
ユニット138へ
送信する
SEED0を用いて
データを
デスクランブル
する
デスクランブル・
ユニット 138
END
保護された環境